**PRÁCTICA N° 5**

Uso de ClamAV como antivirus en Linux

1. **OBJETIVOS**
   1. Entender los conceptos básicos de IDS y cómo funcionan.
   2. Comprender el funcionamiento básico de ClamAV como herramienta de seguridad.
   3. Aprender a instalar y configurar ClamAV en sistemas Linux.
   4. Realizar análisis de archivos y directorios en busca de amenazas.
   5. Analizar y gestionar los registros generados por ClamAV.
2. **MARCO TEÓRICO**
   1. **ClamAV**

ClamAV es un antivirus de código abierto, distribuido bajo la licencia GPL (Licencia Pública General de GNU), desarrollado para identificar diversas amenazas como virus, troyanos, malware y otras actividades maliciosas. Es compatible con múltiples sistemas operativos, incluyendo Windows, GNU/Linux, BSD, Solaris, macOS y otras plataformas basadas en Unix. ClamAV fue creado en 2001 por Tomasz Kojm con el propósito inicial de combatir el malware distribuido a través del correo electrónico. A lo largo de los años, la colaboración de empresas, universidades y organizaciones ha permitido que ClamAV desarrolle una sólida y amplia red de distribución a nivel global.

Por otra parte, las características principales de ClamAV son:

* **Integración con servidores de correo:** Es una herramienta popular en servidores de correo para escanear y filtrar correos electrónicos en busca de contenido malicioso.
* **Motor antivirus:** ClamAV incluye un motor antivirus eficiente para el escaneo de archivos, ofreciendo protección en tiempo real en sistemas Linux mediante su módulo ClamOnAcc.
* **Actualizaciones frecuentes:** Su base de datos de firmas de virus se actualiza constantemente, asegurando la capacidad de detectar las amenazas más recientes.
* **Compatibilidad extensa:** Es compatible con una amplia gama de formatos de archivo, incluyendo archivos comprimidos como ZIP y RAR, así como documentos en formatos PDF y RTF.
* **Interfaz de línea de comandos:** Ofrece herramientas para realizar escaneos bajo demanda desde la línea de comandos, lo que facilita su uso en scripts y procesos automatizados.

1. **TRABAJO PREPARATORIO**
   1. Consultar que es antivirus, su funcionamiento, y las principales clases de amenazas como virus, malware, etc.
   2. Indicar que es ClamAV, su propósito y capacidades.
   3. Explicar la diferencia entre clamscan y clamdscan.
   4. Consultar el funcionamiento de crontab para programar tareas.
2. **EQUIPO Y MATERIALES**

* Oracle VM Virtual Box o VMWare Player.
* Máquina virtual con distribución Ubuntu/Debian que actúe como dispositivo Linux.
* Internet.

1. **PROCEDIMIENTO**

**Instalación de la ClamAV**

* Se instala ClamAV con sus herramientas relacionadas con el siguiente comando sudo apt install -y clamav clamav-daemon. Después se verifica la versión del programa con el comando clamscan –-version.

**Configuración de ClamAV**

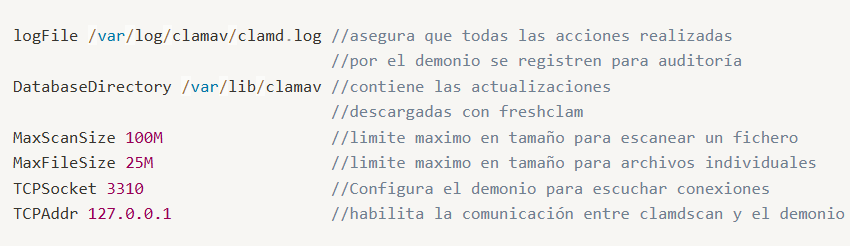
* Primero se debe detener el servicio para actualizar la base de datos de virus de ClamAV con el comando sudo systemctl stop clamav-freshclam, luego para realizar la actualización se utiliza el comando sudo freshclam. Despues se inicia el servicio con el comando sudo systemctl start clamav-freshclam.

A computer code with text

Description automatically generated with medium confidence

Además, con el comando sudo systemctl enable clamav-freshclam el servicio se inicia forma automática cuando arranque el sistema.

* Se edita el archivo de configuración con el comando sudo nano /etc/clamav/clamd.conf, para personalizar el comportamiento de la siguiente forma para este caso.



* Luego de editar el archivo se comprueba que no exista ningún error con el siguiente comando sudo systemctl status clamav-daemon, y a la vez conocer el estado del servicio.

**A computer screen shot of a program

Description automatically generated**

**Automatización de Escaneos con Crontab**

* Por otro lado, se crea una tarea con crontab para realizar escaneos diarios a las 17:00 horas con clamav. El archivo cron se configura de la siguiente forma con el comando crontab -e.

A screen shot of a computer

Description automatically generated

* Por último, con el comando crontab -l, se verifica la configuración de la tarea la cual se ejecutará cada día para monitorear el sistema.

A screenshot of a computer program

Description automatically generated

1. **INFORME**
   1. Documentar las configuraciones aplicadas.
   2. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.
   3. Configurar ClamAV con sistemas como SpamAssassin para escanear correos electrónicos.
2. **REFERENCIAS**

**[1] "Installing and configuring ClamAV in Ubuntu" transip. https://www.transip.eu/knowledgebase/1898-installing-and-configuring-clamav-ubuntu (accessed Jan 12. 2025).**